CONSTRUCTION OF QUASIGROUPS USING THE SINGULAR DIRECT PRODUCT

CHARLES C. LINDNER

ABSTRACT. The idea of a discrete $w(x, y) = v(x, y)$ quasigroup is given along with a generalization of A. Sade's singular direct product. These notions are then used to construct certain types of quasigroups. In particular an algebraic generalization of E. H. Moore's construction of Steiner triple systems is obtained.

1. Introduction. In [5] A. Sade gives a construction for quasigroups which he calls the singular direct product. In [2] this construction is generalized and used to construct quasigroups orthogonal to their transposes. In this paper we give a different generalization of the singular direct product and use this construction to obtain some general results on the constructability of certain types of quasigroups. These results are an improvement on the results obtained in [3]. One of the consequences of our results is an algebraic generalization of Moore's construction for Steiner triple systems [4]. All quasigroups considered in this paper will be finite.

2. Preliminaries. Let $(V, \odot)$ be an idempotent quasigroup and Q a set. For each $v \in V$ let $\circ(v)$ be a binary operation on Q so that $(Q, \circ(v))$ is a quasigroup. Further, suppose that $P \subseteq Q$ is such that all of the operations $\circ(v)$ agree on P and that $(P, \circ(v))$ is a subquasigroup of $(Q, \circ(v))$. Let $\otimes$ be a binary operation on $P' = Q \setminus P$ so that $(P', \otimes)$ is a quasigroup. On the set $P \cup (P' \times V)$ define a binary operation $\oplus$ as follows:

- (1) $p_1 \oplus p_2 = p_1 \circ(v) p_2 = p_1 \circ(w) p_2, \quad \text{if } p_1, p_2 \in P,$
- (2) $p \oplus (p', v) = (p \circ(v) p', v), \quad p \in P, p' \in P', v \in V,$
- (3) $(p', v) \oplus p = (p' \circ(v) p, v), \quad p \in P, p' \in P', v \in V,$
- (4) $(p', v) \oplus (p'', v) = p' \circ(v) p'', \quad \text{if } p' \circ(v) p'' \in P,$
 $\quad = (p' \circ(v) p'', v), \quad \text{if } p' \circ(v) p'' \in P',$
- (5) $(p', v) \oplus (p'', w) = (p' \otimes p'', v \odot w), \quad \text{if } v \neq w.$

Presented to the Society, November 20, 1970; received by the editors September 29, 1970.

AMS 1969 subject classifications. Primary 2095; Secondary 0530.

Key words and phrases. Quasigroups, discrete $w(x, y) = v(x, y)$ quasigroups, Steiner quasigroups, singular direct product.

Copyright © 1971, American Mathematical Society

The quasigroup so constructed will be denoted by $V \times Q(o(v), P, P' \otimes)$. The singular direct product defined here differs from the singular direct product as defined by Sade [5] in that Sade's construction has $o(v) = o(w)$ for all v, w in V . We will denote Sade's singular direct product by $V \times Q(o(v) = o(w), P, P' \otimes)$.

The following notions will be necessary for what follows. They can be found in [3].

Let F be the free groupoid on two generators x and y . The *components* of a word $w(x, y)$ of F are defined by:

(1) if the length of $w(x, y)$ is 1, the only component of $w(x, y)$ is $w(x, y)$, and

(2) if the length of $w(x, y)$ is ≥ 2 , the components of $w(x, y)$ are $w(x, y)$ and the components of $u(x, y)$ and $v(x, y)$, where $w(x, y) = u(x, y)v(x, y)$.

Let Q be a quasigroup such that if $t(x, y) = t_1(x, y)t_2(x, y)$ is any component of $w(x, y)$ of length at least 2 and $a \neq b$ are any two elements of Q , then $t_1(a, b) \neq t_2(a, b)$. Such a quasigroup is called a *discrete* $w(x, y)$ -quasigroup. If Q is a discrete $w(x, y)$ and $v(x, y)$ -quasigroup and satisfies the identity $w(x, y) = v(x, y)$, Q is called a *discrete* $w(x, y) = v(x, y)$ -quasigroup.

3. Construction of quasigroups using the singular direct product $V \times Q(o(v), P, P' \otimes)$.

THEOREM 1. *The singular direct product $V \times Q(o(v), P, P' \otimes)$ as given in the definition contains an isomorphic copy of each of the quasigroups $(Q, o(v))$ and at least as many copies of $(V, \odot)$ as there are idempotents in $(P', \otimes)$ which are also idempotent in each of $(Q, o(v))$. Furthermore, $V \times Q(o(v), P, P' \otimes)$ has order $v(q-p) + p$, where $v = |V|$, $q = |Q|$, and $p = |P|$.*

PROOF. For each $v \in V$, $(P \cup (P' \times \{v\}), \oplus)$ is isomorphic to $(Q, o(v))$. Similarly if $p' \in P'$, $p' \otimes p' = p'$, and $p' \circ(v) p' = p'$ for all $v \in V$, then $(\{p'\} \times V, \oplus)$ is isomorphic to $(V, \odot)$.

THEOREM 2. *If $(V, \odot)$ is idempotent and a discrete $w(x, y) = v(x, y)$ quasigroup, $(Q, o(v))$ satisfies $w(x, y) = v(x, y)$ for all $v \in V$, and $(P', \otimes)$ satisfies $w(x, y) = v(x, y)$, then $V \times Q(o(v), P, P' \otimes)$ satisfies $w(x, y) = v(x, y)$. Furthermore, $V \times Q(o(v), P, P' \otimes)$ contains a copy of each of $(Q, o(v))$ and at least as many copies of $(V, \odot)$ as there are idempotents in $(P', \otimes)$ which are also idempotents in each of $(Q, o(v))$. Furthermore, $V \times Q(o(v), P, P' \otimes)$ has order $v(q-p) + p$, where $v = |V|$, $q = |Q|$, and $p = |P|$.*

PROOF. Let $a, b \in P \cup (P' \times V)$. If $a, b \in P \cup (P' \times \{v\})$ for some $v \in V$, since $(P \cup (P' \times \{v\}), \oplus)$ is isomorphic to $(Q, \circ(v))$ we have $w(a, b) = v(a, b)$ immediately. If $a = (p', v)$ and $b = (p'', w)$ where $v \neq w$, the proof that $w(a, b) = v(a, b)$ is identical to the corresponding case in the proof of Theorem 1 in [3]. This shows that $V \times Q(\circ(v), P, P' \otimes)$ satisfies $w(x, y) = v(x, y)$. The remainder of Theorem 2 follows from Theorem 1.

4. Construction of Steiner quasigroups. In [3] the question was raised as to whether the singular direct product could be used to construct Steiner quasigroups of all orders $\equiv 1$ or $3 \pmod{6}$. The following theorem shows that this is the case.

THEOREM 3. *Let $(V, \odot)$ be a Steiner quasigroup of order v and for each $v \in V$ let $(Q, \circ(v))$ be a Steiner quasigroup of order q . Further let P be a subset of Q so that all $\circ(v)$ agree on P and $(P, \circ(v))$ is a subquasigroup of $(Q, \circ(v))$. Then there is a Steiner quasigroup of order $v(q-p)+p$ containing a copy of each of $(Q, \circ(v))$ and at least one copy of $(V, \odot)$.*

PROOF. Let $(V, \odot)$, $(Q, \circ(v))$, and $(P, \circ(v))$, all $v \in V$, be as above. Then $(V, \odot)$ is idempotent and both $x(xy) = y$ and $(yx)x = y$ discrete. The same is true for each $(Q, \circ(v))$ —but we only need the fact that each is idempotent and satisfies each of the identities $x(xy) = y$ and $(yx)x = y$. Set $P' = Q \setminus P$ and define $(P', \otimes)$ isomorphic to $(\{0, 1, 2, \dots, n-1\}, \circ)$ where $i \circ j = k$ if and only if $i+j+k \equiv 0 \pmod{n}$. Then $(P', \otimes)$ satisfies both identities $x(xy) = y$ and $(yx)x = y$ and contains at least one idempotent, which is of course idempotent in each of $(Q, \circ(v))$ since each is a Steiner quasigroup. By Theorem 2 $V \times Q(\circ(v), P, P' \otimes)$ has order $v(q-p)+p$, contains copies of all $(Q, \circ(v))$, contains at least one copy of $(V, \odot)$, and satisfies the identities $x(xy) = y$ and $(yx)x = y$. Since $(V, \odot)$ and each $(Q, \circ(v))$ is idempotent so is $V \times Q(\circ(v), P, P' \otimes)$. Hence $V \times Q(\circ(v), P, P' \otimes)$ is a Steiner quasigroup. This completes the proof.

We note that in the statement of Theorem 3 if we take $\circ(v) = \circ(w)$ for all v, w in V , Theorem 3 reduces to the algebraic analogue of Moore's construction for Steiner triple systems [4].

5. Remarks. In [1] J. Doyen proves the following theorem.

Let Q_1, Q_2 , and Q_3 be three Steiner triple systems of the same order such that $Q_1 \cap Q_2 = Q_2 \cap Q_3 = Q_3 \cap Q_1 = P$, where P is a subsystem of order p of Q_1, Q_2, Q_3 . If $q > 3p$, it is possible to con-

struct on the set $Q_1 \cup Q_2 \cup Q_3$ a Steiner triple system Q of order $3q - 2p$ such that Q_1, Q_2, Q_3 are the only subsystems of Q of order q .

Now, Doyen's theorem is the special case of Theorem 3 taking $(V, \odot)$ to be Steiner quasigroup of order 3. Because of this it seems plausible, at least to the author, to make the following conjecture.

CONJECTURE. In the statement of Theorem 3, if $q > vp$, then the only subquasigroups of $V \times Q(o(v), P, P' \otimes)$ of order q are the copies of $(Q, o(v))$ for each $v \in V$.

Doyen uses his theorem to obtain results on the number of non-isomorphic Steiner triple systems of certain orders [1]. Verification of the above conjecture should sharpen these results.

One might also investigate the number of subquasigroups of order q in the statement of Theorem 2.

ADDED IN PROOF. The above conjecture has recently been verified by Tina Straley (Notices Amer. Math. Soc. 17 (1970), 1023).

REFERENCES

1. Jean Doyen, *Sur la croissance du nombre de systèmes triples de Steiner non isomorphes*, J. Combinatorial Theory 8 (1970), 424-441.
2. C. C. Lindner, *The generalized singular direct product for quasigroups*, Canad. Math. Bull. (to appear).
3. C. C. Lindner, *Identities preserved by the singular direct product*, Algebra Universalis 1 (1971), 86-89.
4. E. H. Moore, *Concerning triple systems*, Math. Ann. 43 (1893), 271-285.
5. A. Sade, *Produit direct-singulier de quasigroupes orthogonaux et antiabéliens*, Ann. Soc. Sci. Bruxelles Ser. I 74 (1960), 91-99. MR 25 #4017.

AUBURN UNIVERSITY, AUBURN, ALABAMA 36830